

~~SECRET~~

SENIOR INTERAGENCY GROUP (INTELLIGENCE)  
INTERAGENCY GROUP/COUNTERMEASURES (POLICY)  
WASHINGTON, D.C. 20505

OS REGISTRY

05 AUG 1987

~~SECRET~~ ICS 0911-87  
31 July 1987

MEMORANDUM FOR: IG/CM(P) Members

FROM:   
Executive Secretary

25X1

SUBJECT: Draft Minutes--Eighth IG/CM(P) Meeting, 21 July 1987

Attached for your information is a copy of the draft minutes of the 21 July 1987 IG/CM(P) meeting. If there are corrections, they should be furnished to the Executive Secretariat  by COB 14 August 1987; otherwise the minutes will be considered final.

25X1

25X1

Attachments:  
a/s

Regraded Unclassified upon  
removal of classified attachment

~~SECRET~~

CCISCMO/ICS: [REDACTED] (31 July 1987)

STAT

Distribution of D/ICS 0911-87 (w/atts as shown):

1 - Mr. Alderman, OSD  
1 - Mr. Donnelly, ODUSD(P)  
1 - Mr. Anderson, ODUSD(P)  
1 - Mr. Thomas, ASD C<sup>3</sup>I  
1 - COL Gallo, OACSI, DA  
1 - RADM Flynn, Navy  
1 - Ms. Smith, Air Force  
1 - Mr. Guenther, Marine Corps  
1 - Mr. Seidman, Coast Guard  
2 - [REDACTED] (one for JCS)  
1 - [REDACTED]  
1 - Mr. Penrith, FBI  
1 - Mr. Corry, State  
1 - Mr. Lamb, State (via Mr. Corry)  
1 - Mr. Lewis, NSC  
1 - [REDACTED]  
1 - [REDACTED]  
1 - Ms. Lawton, DoJ  
1 - Mr. Cassetta, Commerce  
1 - Mr. Seaton, Energy (via Mr. Brown)  
1 - Mr. Foss, Treasury  
1 - Mr. Garfinkel, ISOO  
1 - Ms. Sciafani, OPM (HOLD IN CCISCMO/ICS)  
1 - DCI  
1 - ER  
1 - D/ICS (via DD/ICS)  
1 - ICS Registry  
1 - IG/CM subject  
1 - IG/CM chrono

STAT

STAT

UNCLASSIFIED

~~SECRET~~

SUMMARY OF IG/CM(P) MEETING  
21 JULY 1987

ROOM 6W02, [REDACTED]

25X1

1. The eighth meeting of the Interagency Group/Countermeasures (Policy) was convened at 1400 hours, 21 July 1987, by the Chairman, Mr. Craig Alderman, Jr., Deputy Under Secretary of Defense (Policy). A list of individuals attending is at Attachment 1. [REDACTED]

25X1

2. The Chairman made the following opening remarks:

a. Minutes of the seventh IG/CM(P) meeting have been corrected and are now considered final. [REDACTED]

25X1

b. Members are reminded that an effort is made to establish the date of the next IG/CM(P) meeting in the penultimate paragraph of the minutes of each meeting for planning purposes, however, as with this meeting, there are times when the planned date must be changed. Again as a reminder IG/CM(P) members will be provided an independent announcement and agenda prior to the actual meeting date. If you have not received the independent announcement prior to the planned scheduled date for the meeting it is recommended you contact the Secretariat at [REDACTED]

25X1

25X1

3. The scheduled agenda was addressed with the following results:

a. LOCK INITIATIVE UPDATE:

(1) The Chairman, IG/CM(P), informed the group members that several of the committee's previously planned actions regarding the lock initiative have occurred since the last meeting. To begin with the Chairman, SIG-I, as requested, was provided with a copy of the agreed upon revised press guidance regarding the lock initiatives. The public affairs guidance (Attachment 2) has been dispatched to the appropriate agencies. It is to be used in responding to queries that may arise in regard to questions pertaining to US security equipment. It is anticipated that questions may stem from an expected announcement in the Federal Register indicating a change in ISOO Directive #1 concerning national security, or the recent GSA and Department of State discussions with lock manufacturer representatives on reviewing the possible need to enhance

25X1

~~SECRET~~

the current three-position combination locking system presently used by all government agencies. The guidance is provided specifically for action by the GSA Public Affairs Office and for the information of all other addressees. ☐

25X1

(2) The Director of the Information Security Oversight Office (ISOO), as recommended by the group at the last meeting (IG/CM[P] minutes of 12 May 1987) forwarded to the National Security Council the proposed change to ISOO Directive No. 1 (Attachment 3). ☐

25X1

(3) Per the request of the group members (IG/CM[P] minutes of 12 May 1987) the Director of ISOO has forwarded an advisory letter (Attachment 4) to some seventy senior government officials. The letter advises them of the potential vulnerability of the combination lock security containers to the new and emerging technological developments; apprising them of actions they may take to address the issue; and alerting them to consider supplemental precautionary measures that we believe will enhance the protection of national security information. ☐

25X1

(4) The Chairman, IG/CM(P), has informed the Select Committee on Intelligence, United States Senate, and the Permanent Select Committee on Intelligence, U.S. House of Representatives, of the background and initiatives under way addressing the circumstances of the lock initiatives which have, in part, significant physical security implications. ☐

25X1

(5) The DUSP(P) requested GSA to provide the Naval Civil Engineering Laboratory with \$250K to \$350K for twelve months operating costs to continue its work toward both assessing the viability of current combination lock standards and developing new locks to counter present vulnerabilities. ☐

25X1

ACTION: The Physical Security Committee (PhySC) continue monitoring the ongoing combination lock actions being initiated by both IACSE and NCEL. Provide the Chairman, IG/CM(P), with a status report at the next scheduled meeting. ☐

25X1

b. Howard Case post-Brief: [ ] Director, Office of Security, Central Intelligence Agency, informed the group members that Mr. Carlucci, National Security Advisor, requested CIA to share their newly revised post-Howard personnel and security measures with the entire Intelligence Community in order to determine their applicability to other agencies. [ ] indicated that he was pleased to be able to discuss the subject matter with the group members and personally felt sharing such information to other intelligence agencies within the government was beneficial to all. [ ]

25X1

25X1

25X1

25X1

In summary, [ ] indicated that the Howard case highlighted the following major needs:

25X1

(1) Greater coordination among CIA components responsible for security, personnel, and medical processing of applicants.

(2) Greater coordination between CIA and the FBI on cases of counterintelligence concern.

(3) Greater attention to the attitudes of employees separated from CIA.

(4) Better post-employment tracking of separated employees. [ ]

25X1

[ ] informed the group that since the Howard incident the following positive steps have been taken to meet all of the needs highlighted in the above findings:

25X1

(1) New inter-component panels have been formed, and the role of an existing panel expanded, to facilitate sharing of relevant security, personnel, and medical information and the proper use of such information in the hiring and clearance decision process.

(2) By means of a newly developed memorandum of agreement between the FBI and the CIA better coordination has been effected for the passing of information which indicates the possibility of a potential espionage case.

(3) The manner in which employees are now separated from CIA has been largely revamped with a much greater focus on assessing the threat posed by employees. Employees determined to be a potential risk to national security are separated from the agency in a manner designed to prevent resentment and vindictiveness.

(4) Expanded systems have been developed, consistent with applicable law and regulation, to identify former employees who may be high risk and to better track them and, as appropriate, attend to individual needs for guidance and support. ☐

25X1

☐ informed the group that information pertaining to Mr. Howard's behavior was developed during a periodic reevaluation conducted prior to the end of his three-year trial period of employment. As a result, he was offered and accepted the opportunity to resign. ☐

25X1

25X1

ACTION: Each member in the IG/CM(P) is requested to review the measures discussed by the CIA for suitability for application within their own agency. It is requested that once the review has been accomplished that each agency then forward a written summary of how personnel security problems are identified to the Chairman, Physical Security Committee, IG/CM(P), by 27 August 1987. If during the review an agency finds suitability for application of any of the methodology presented that also should be provided in the summary report. ☐

25X1

4. Other Old Business There was no old business to discuss. ☐

25X1

5. New Business: ☐ Chairman, Personnel Security Committee (PSC), IG/CM(P), advised the group that the PSC has been tasked with an action item contained in the President's report to Congress regarding notification of foreign travel before departure by cleared personnel. The PSC has prepared a survey (Attachment 5) to collect data from group members on how they are currently handling the reporting requirement of foreign travel by cleared personnel. The PSC Chairman requested that each group member take a copy of the survey and return the survey to his committee by 28 August 1987. ☐

25X1

25X1

ACTION: Each IG/CM(P) member complete the Survey of Foreign Travel Reporting Requirements and return it to the PSC by 28 August 1987. ☐

25X1

6. Next Meeting: The Chairman announced that the next meeting of the IG/CM(P) is tentatively scheduled for the last week in August or first week in September. ☐

25X1

7. Adjournment: The meeting adjourned at 1530 hours. ☐

25X1

CONFIDENTIAL

Attachment 1

**ATTENDEES**  
**IG/CM(P) MEETING, 12 MAY 1987**  
**ROOM 6W02, COMMUNITY HEADQUARTERS BUILDING**

<u>NAME</u>	<u>ORGANIZATION</u>	
ALDERMAN, Craig	OSD	
ALLEN, Robert C.	Navy	
		25X1
ANDERSON, Maynard	OSD	
		25X1
BUJAC, Gregory	State	
CASSETTA, Michael	Commerce	
CONNELL, George M.	Navy	
CORRY, Frank	State	
DIETRICH, Patrick J.	Coast Guard	
DONNELLY, John F.	OSD	
		25X1
GALLO, Anthony	Army	
GARFINKEL, Steven	IS00	
GUENTHER, John	Marine Corps	
HOOVER, John	OSD	
KONDURIS, Ted	Air Force	
LANNON, James W.	State	
LAWTON, Mary	Justice	
		25X1
McMENEMIN, Robert	Treasury	
		25X1
PASEUR, George	Air Force	
		25X1
PENRITH, Gary	FBI	
		25X1
RUBINO, D. Jerry	Justice	
SCHWARTZ, Louis	State	
SCLAFANI, Frances	OPM	
		25X1
TEMPLE, Albert Don	DoE	
THOMAS, Jack E.	OSD	
		25X1

CONFIDENTIAL

~~SECRET~~ATTACHMENT 2SENIOR INTERAGENCY GROUP (INTELLIGENCE)  
INTERAGENCY GROUP/COUNTERMEASURES (POLICY)  
WASHINGTON, D.C. 20505

DCI/ICS 0896-87

6 JUL 1987

MEMORANDUM FOR: Distribution

FROM: Craig Alderman, Jr.  
ChairmanSUBJECT: Public Affairs Guidance ☐

25X1

1. The Interagency Group for Countermeasures Policy [IG/CM(P)], a subelement of the Senior Interagency Group-Intelligence, has recently been deliberating on a significant physical security issue as outlined in paragraph two below. A number of actions resulting from those deliberations may cause further inquiry from the media. Accordingly, the IG/CM(P) has developed public affairs guidance for use as required (Attachment 1). Consistent with paragraph four below, the guidance is provided specifically for action by the GSA Public Affairs Office and for the information of all other addressees. ☐

25X1

2. The Interagency Advisory Committee on Security Equipment (IACSE), chaired by the General Services Administration (GSA), sponsored a study on the manipulation resistance of GSA-approved, three-position combination locks. Three independent contractors tested such combination locks manufactured by Mosler, LaGard, and Sargent and Greenleaf. The results of the tests showed that recent advances in technology could be used to defeat these combination locks surreptitiously, effectively reducing the degree of lock protection provided. The current GSA standard requires 20 hours of delay against manipulation. The use of computers and other technically enhanced manipulation techniques permitted penetration within two to four hours. ☐

25X1

3. The attached public affairs guidance is to be used in responding to queries that may arise in regard to questions pertaining to US security equipment. It is anticipated that questions may stem from an expected announcement in the Federal Register indicating a change in IS00 Directive #1 concerning national security (Attachment 2), or anticipated GSA discussions with lock manufacturer representatives on reviewing the possible need to enhance the current three-position combination locking system presently used by all government agencies. ☐

25X1

Regrade Confidential when  
separated from Secret attachment ☐

25X1

~~SECRET~~




SECRET

SUBJECT: Public Affairs Guidance ☐

25X1

4. The GSA has agreed to respond for the government to any public inquiries regarding the subject matter in the above paragraph. Therefore, it is requested that all such inquiries be referred to the GSA Public Affairs Office. ☐

25X1

  
Craig Alderman, Jr.

Attachments:  
a/s

SECRET

~~SECRET~~ATTACHMENT 1PUBLIC AFFAIRS GUIDANCE

The following public affairs guidance is for use in a response on a query basis only to questions pertaining to changes to ISOO Directive #1 on national security information. This will shortly appear in the Code of Federal Regulations. Federal Agencies and the DoD will refer questions on the directive to public affairs in the appropriate Federal Agency.

DRAFT PRESS GUIDANCE

Recent reviews by interagency committees responsible for security equipment have found that physical security programs have not in all cases kept pace with improvements in technology. These improvements include both the technology available to adversaries, whether terrorists or hostile intelligence services, and protective systems used to prevent or deter operations against Federal Government assets. A coordinated effort is underway to update and upgrade security standards and practices in general. As research and development efforts reach fruition and analyses of incidents are completed, you will see evidence of improvements. New policies, procedures, and equipment specifications will change the way we protect personnel, equipment, and information. The recent change to the Information Security Oversight Office Directive #1 is one of many examples within the Government. We are attempting to apply new technology in a cost-effective manner to reduce risks to national assets.

UNTIL APPROVED FOR DISSEMINATION  
THIS PRESS GUIDANCE SHOULD BE CONSIDERED CLASSIFIED--SECRET

~~SECRET~~  
DECL:OADR

SECRET

1. Q: You mentioned the change to the security directive in the CFR, give us some other examples?  
A: We plan to update testing standards and change Federal Specifications for security containers and combination locks, for example.
2. Q: Is this related to any of the on-going espionage investigations?  
A: No, these efforts preceded the recent publicity; however, this has provided justification for increased attention in this area.
3. Q: Why can't this process be accelerated?  
A: We are operating under fiscal constraints, which allow only a limited number of upgrades to be completed annually.

UNTIL APPROVED FOR DISSEMINATION  
THIS PRESS GUIDANCE SHOULD BE CONSIDERED CLASSIFIED--SECRET

SECRET  
DECL:OADR

SUBJECT: Public Affairs Guidance

25X1

CCISCMO/ICS:  (6 July 1987)

25X1

Distribution of DCI/ICS 0896-87 (w/atts)

- 1 - Derek J. Vander Schaff, Deputy IG, DoD
- 1 - , D/PAO, CIA
- 1 - Sherman M. Funk, IG-Designate, State
- 1 - Paul Costello, D/PAO, GSA
- 1 - Steven Garfinkel, D/IS00
- 1 - ICS Registry
- 1 - IG/CM(P) chrono
- 1 - IG/CM(P) subject

25X1

ATTACHMENT 3



Information Security Oversight Office  
Washington, DC 20405

July 6, 1987

MEMORANDUM FOR: The Honorable  
Grant S. Green, Jr.  
Staff Secretary, National Security Council

FROM: Steven Garfinkel *Steven Garfinkel*  
Director, Information Security Oversight Office

SUBJECT: Proposed change to ISOO Directive No. 1

Under Executive Order 12356, "National Security Information," the Information Security Oversight Office (ISOO) is required to receive the approval of the National Security Council (NSC) before issuing or amending an ISOO directive that impacts on all agencies that create or handle classified information. With the concurrence of the member agencies of the Interagency Group/Countermeasures (Policy) and the Director of Central Intelligence, ISOO proposes to amend § 2001.43 of its Directive No. 1 (32 CFR Part 2001) to enhance the minimum safeguarding requirement for TOP SECRET information that is stored outside the United States. David Major of the NSC staff is familiar with the factors that have led us to conclude that an enhancement is necessary at this time. We enclose the pertinent portion of the proposed section, with the new language underlined, as an appendix to this memorandum. As soon as we have received the NSC's concurrence, we will proceed with its effectuation through publication in the Federal Register.

Enclosure

APPENDIX: Proposed Change to ISOO Directive No. 1

§ 2001.43 Storage

\*

\*

\*

(a) Minimum requirements for physical barriers.  
(1) Top Secret. Top Secret information shall be stored in a GSA-approved security container with an approved, built-in, three-position, dial-type changeable combination lock; in a vault protected by an alarm system and response force; or in other types of storage facilities that meet the standards for Top Secret established under the provisions of § 2001.41. For Top Secret information stored outside the United States, one or more of the following supplementary controls is required:  
(i) the area that houses the security container or vault shall be subject to the continuous protection of guard or duty personnel; (ii) guard or duty personnel shall inspect the security container or vault at least once every two hours; or (iii) the security container or vault shall be controlled by an alarm system to which a force will respond in person within 15 minutes. In addition, heads of agencies shall prescribe those supplementary controls deemed necessary to restrict unauthorized access to areas in which such information is stored.

~~CONFIDENTIAL~~

ATTACHMENT 4



Information Security Oversight Office  
Washington, DC 20405

ISOO-C-87-011

July 6, 1987

Dear Mr. Alderman:

(C) This is an advisory notice regarding security containers. It is intended to advise you of the potential vulnerability of combination lock security containers to new and emerging technological developments; to apprise you of actions being taken to address this issue; and to alert you to consider supplemental precautionary measures that we believe will enhance the protection of national security information.

(U) A number of years ago it was decided among the agencies that are significantly involved in the safeguarding of national security information that combination locks, to be acceptable for this purpose, must protect against surreptitious entry for at least 20 consecutive man-hours. Surreptitious entry refers to the compromise of a security container without leaving physical evidence that the container has been compromised, e.g., manipulating the lock to reveal its combination. Group 1 and Group 1-R combination locks currently used for the protection of national security information were approved on the basis that, among other standards, they would provide the 20 man-hours of protection against surreptitious entry.

(C) Current technologies may have rendered the 20 man-hour standard for Group 1 and Group 1-R locks obsolete. These new technologies are now packaged in devices that are commercially available, relatively inexpensive and easily concealed. While studies of the matter are continuing, some preliminary findings

Classified by: Director, ISOO  
Declassify on: OADR

~~CONFIDENTIAL~~

CONFIDENTIAL

-2-

indicate that the degree of protection provided by combination locks against surreptitious entry can, through the application of current technology, be diminished to four man-hours or less. Responsible executive branch agencies are currently working to establish conclusively the vulnerability of the current locks, and, as appropriate, develop interim technical countermeasures; to consider anew the appropriate standard for protection against surreptitious entry; and to develop specifications for locks that will meet this and other existing standards. The completion of these tasks may not come quickly.

(C) Following consultation with the member agencies of the Interagency Group/Countermeasures (Policy), the Information Security Oversight Office (ISOO) is now seeking the approval of the National Security Council to enhance the minimum safeguard requirements for Top Secret information stored outside the United States, where the threat from this new vulnerability is believed to be much greater. We enclose a copy of the proposed language. Storage standards published in ISOO Directive No. 1 (32 CFR Part 2001) establish the minimum acceptable levels of protection for classified information. Agencies are always encouraged to establish, by internal regulation, more stringent standards for information under their control.

(C) At present, there are no immediate plans to mandate enhanced minimum storage requirements for national security information within the United States. Until such time as new lock and storage standards are developed and implemented, however, your agency should take those precautionary measures that are feasible without a massive expenditure of additional resources. You should notify appropriate officials within your agency of the increased threat to properly stored classified information; survey your particular threat situations; and, where feasible, protect classified information, especially highly sensitive information, through the application of supplemental countermeasures. For example, in locations where Top Secret information is dispersed, you may wish to consolidate the material in an approved container or vault protected by on-site personnel or an alarm system and response force; or to introduce any other supplemental control that enhances the minimal protection requirements for classified material at that level and below. A classified records clean-out campaign, which disposes of and consolidates classified holdings, is another inexpensive means to reduce the vulnerability. In the course of its program reviews, ISOO will examine those steps that you have taken in response to the increased vulnerability.

CONFIDENTIAL



CONFIDENTIAL

-3-

(C) The details concerning the vulnerabilities of the Group 1 and Group 1-R locks are classified at the Secret level. This information must be protected accordingly.

(U) If you desire further information, please contact Rudolph Waddy, ISOO Program Analyst, or me at 535-7251 (non-secure). If we do not know the answer to your specific question, we will attempt to put you in touch with someone who does.

Sincerely,

~~(Signed)~~ Steven Garfinkel

Steven Garfinkel  
Director

Mr. Craig Alderman, Jr.  
Deputy Under Secretary of Defense (Policy)  
Room 2E812, The Pentagon  
Washington, DC 20301-2200

Enclosure

CONFIDENTIAL

ATTACHMENT 5

MEMORANDUM FOR: Members, IG/CM(P)

FROM:

Chairman, Personnel Security Committee

STAT

SUBJECT: Survey of Foreign Travel Reporting Requirements

1. The Personnel Security Committee (PSC) of the IG/CM(P) has been tasked with action on an item contained in the President's Report to Congress which reads:

Require that all cleared employees (including contractors) notify the security office of their respective agencies of all personal foreign travel before departure.

2. As a first step, we are surveying agencies to determine what is currently being done and to assist the Security Awareness and Education Subcommittee of the PSC in developing from that base a model which agencies can adapt to their needs. The model will identify basic elements which all programs should have as well as optional suggestions for reporting channels, records keeping, guidance and briefing for travelers, etc. We plan to start with procedures for government agencies then see how those procedures might be fitted to the contractor environment.

3. Members are requested to complete the attached survey prior to the next meeting of the IG/CM(P) and return it at that meeting or send it to the Executive Secretary, Personnel Security Committee, CIA, Washington D.C. 20505.

STAT

FOR OFFICIAL USE ONLY

## FOREIGN TRAVEL REPORTING SURVEY

Where responses require narrative comments, please attach papers with responses keyed to the numbered items below. Lines are provided below where short answers are likely to suffice. Please do not feel limited by the questions - further exposition, explanation, suggestion or other comments are welcome. We are searching not only for good techniques but also for basic elements, constraints, limitations, applications, and problems agencies might encounter in complying with the President's Report requirement.

1. Do you require reporting by all accessed employees:  
of all foreign travel? \_\_\_\_\_  
in advance of travel? \_\_\_\_\_  
mandatory? \_\_\_\_\_
2. If not, what are the exceptions and why? Do you require reporting only by those with access to Sensitive Compartmented Information as required by DCID 1/20?
3. What is the regulatory basis for your reporting requirement? Please attach copy (if other than DCID 1/20).
4. How are employees advised of their obligation to report?
5. From your experience, can you suggest any regulatory or procedural areas which should be given particular attention to ensure compliance?
6. Are employees overseas treated differently in any essential ways than those in U.S.? \_\_\_\_\_ If so, why?
7. What is vehicle for reporting? Memo? Form?  
Please attach copies or exemplar.
8. What information is reported?
9. Who reviews the report? (supervisor? security professional? counterintelligence officer? security education officer?) Who has final approval authority?
10. What is response of security or other authority? Is employee advised of permission to travel? Is employee briefed on: how to act in denied areas? \_\_\_\_\_ Harassments and provocations? \_\_\_\_\_ General travel advice? \_\_\_\_\_ Risk of Capture? \_\_\_\_\_ Counterterrorism? \_\_\_\_\_ Personal protection? \_\_\_\_\_ Other? \_\_\_\_\_

FOR OFFICIAL USE ONLY

11. Where is the report filed? Is it kept with other security and counterintelligence related files? Is it made available to other agencies conducting a National Agency Check? How long is it kept?

12. Is it reviewed in the event of periodic reinvestigation or other security incident or review?

13. Listed below are some possible elements all programs should contain. Please indicate in margin below your agreement or disagreement - (please explain any "disagrees"). Your responses are for our guidance only - not an official position. Please add any comments as you like or suggest other elements you believe should be basic to all programs:

- a. All accessed employees report
- b. Reporting done in advance
- c. All travel is reported
- d. Reports go to professional security official or counterintelligence official for review
- e. Reports stored in such a manner that they are available for review on occasion of all security actions (reinvestigation, NAC, change of clearance status, incident, etc.)
- f. All accessed employees receive foreign travel security awareness briefing as part of regular security awareness program and/or an annual reminder of the reporting requirement.
- g. Employees contemplating travel to hostile areas receive comprehensive defensive briefing for the specific area of intended travel as close as possible to such travel but no longer than one year prior to each trip.
- h. Employees required to report noteworthy incidents to U.S. Consul, Attache, RSO or post Duty Officer in country of travel and to security official upon return.

YOUR ASSISTANCE IS VERY MUCH APPRECIATED  
PLEASE RETURN SURVEY TO

EXECUTIVE SECRETARY, PERSONNEL SECURITY COMMITTEE,  
CIA, WASHINGTON, D.C. 20505

FOR OFFICIAL USE ONLY